

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

ANAMARI LAURENTZ, *individually and on
behalf of all others similarly situated,*

Plaintiff,

v.

ADVANCED RECOVERY EQUIPMENT AND
SUPPLIES LLC,

Defendant.

Case No. _____

CLASS ACTION

DEMAND FOR JURY TRIAL

CLASS ACTION COMPLAINT

Plaintiff Anamari Laurentz (“Plaintiff”), individually and on behalf of all others similarly situated (“Class Members”), brings this Class Action Complaint against Defendant Advanced Recovery Equipment and Supplies LLC (“Defendant”), alleging as follows based upon personal knowledge, information and belief, and investigation of counsel.

NATURE OF THE ACTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard Plaintiff’s and Class Members’ sensitive personally identifiable information (“PII”)¹ and personal health information (“PHI”), which, as a result, is now in criminal cyberthieves’ possession.

2. In June and July 2023, hackers targeted and accessed Defendant’s network systems and stole Plaintiff’s and Class Members’ sensitive, confidential PII and PHI stored therein,

¹ The Federal Trade Commission (“FTC”) defines “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, Social Security number, date of birth. . . .” 17 C.F.R. § 248.201(b)(8).

including their names, street addresses, email addresses and/or phone number(s), Social Security numbers, dates of birth, driver's license or state-issued identification numbers, credit or debit card numbers or information, usernames and passwords associated with online accounts, health insurance policy information, medical diagnosis and treatment information, and other sensitive data (collectively, "Private Information"), causing widespread injuries to Plaintiff and Class Members (the "Data Breach").

3. Defendant is a healthcare provider furnishing durable medical equipment and supplies and related services ("DMES") to patients throughout the Tri-State Area and beyond.²

4. Plaintiff and Class Members are current and former patients of Defendant who, in order to obtain DMES from Defendant, were and are required to entrust Defendant with their sensitive, non-public Private Information. Defendant could not perform its operations or provide its services without collecting Plaintiff's and Class Members' Private Information and retains it for many years, at least, even after the patient-provider relationship has ended.

5. Healthcare providers like Defendant that handle Private Information owe the individuals to whom that data relates a duty to adopt reasonable measures to protect such information from disclosure to unauthorized third parties, and to keep it safe and confidential. This duty arises under contract, statutory and common law, industry standards, representations made to Plaintiff and Class Members, and because it is foreseeable that the exposure of Private Information to unauthorized persons—and especially hackers with nefarious intentions—will harm the affected individuals, including but not limited to by the invasion of their private health matters.

² See *About Us*, Advanced Recovery Equip. and Supplies, <https://advancedrecoveryequipment.com/about-us/> (last visited Nov. 4, 2024).

6. Defendant breached these duties owed to Plaintiff and Class Members by failing to safeguard their Private Information it collected and maintained, including by failing to implement industry standards for data security to protect against, detect, and stop cyberattacks, which failures allowed criminal hackers to access and steal approximately 56,000 patients' Private Information from Defendant's care.

7. According to Defendant's notice of the Data Breach posted on its website, an unknown, unidentified hacker had "unauthorized access" to Defendant's information technology ("IT") network from June 27–July 28, 2023, and accessed and exfiltrated files containing patients' Private Information stored therein.

8. Although the Data Breach took place in June and July 2023, Defendant failed to detect, investigate, or determine that Plaintiff's and Class Members' Private Information has been compromised in the Data Breach until September 29, 2024—over a year after the Data Breach occurred—evidencing Defendant's failure to implement industry-standard logging, monitoring, and alerting systems that would have notified it of the unauthorized access when it occurred.

9. Moreover, Defendant failed to notify affected individuals that their Private Information was compromised until October 2024—over 15 months after the Data Breach—diminishing Plaintiff's and Class Members' ability to timely and thoroughly mitigate and address the increased and imminent risk of identity theft and other harms the Data Breach caused.

10. Defendant failed to adequately protect Plaintiff's and Class Members' Private Information—and failed to even encrypt or redact this highly sensitive data. This unencrypted, unredacted Private Information was compromised due to Defendant's negligent and/or careless acts and omissions and its utter failure to protect its patients' sensitive data.

11. Defendant maintained the Private Information in a reckless manner. In particular,

Private Information was maintained on and/or accessible from Defendant's network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus, Defendant knew that failing to take reasonable steps to secure the Private Information left it in a dangerous condition.

12. Hackers targeted and obtained Plaintiff's and Class Members' Private Information from Defendant's network because of the data's value in exploiting and stealing identities. As a direct and proximate result of Defendants' inadequate data security and breaches of its duties to handle Private Information with reasonable care, Plaintiff's and Class Members' Private Information has been accessed by hackers and exposed to an untold number of unauthorized individuals. The present and continuing risk to Plaintiff and Class Members as victims of the Data Breach will remain for their respective lifetimes.

13. The harm resulting from a cyberattack like this Data Breach manifests in numerous ways including identity theft and financial fraud, and the exposure of an individual's Private Information due to a data breach ensures that the individual will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of his or her life. Mitigating that risk, to the extent it is even possible to do so, requires individuals to devote significant time and money to closely monitor their credit, financial accounts, and email accounts, and take several additional prophylactic measures.

14. As a result of the Data Breach, Plaintiff and Class Members suffered and will continue to suffer concrete injuries in fact, including but not limited to (a) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (c)

actual identity theft and fraud; (d) financial costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) deprivation of value of their Private Information; (g) loss of privacy; (h) emotional distress including anxiety and stress in with dealing with the Data Breach; and (i) the continued risk to their sensitive Private Information, which remains in Defendant's possession and subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect the patient data it collects and maintains.

15. To recover from Defendant for these harms, Plaintiff, on his own behalf and on behalf of the Class as defined herein, brings claims for negligence/negligence *per se*, breach of implied contract, breach of confidence, and unjust enrichment, to address Defendant's inadequate safeguarding of Plaintiff's and Class Members' Private Information in its care.

16. Plaintiff and Class Members seek damages and equitable relief requiring Defendant to (a) disclose the full nature of the Data Breach and types of Private Information exposed; (b) implement data security practices to reasonably guard against future breaches; and (c) provide, at Defendant's expense, all Data Breach victims with lifetime identity theft protection services.

PARTIES

Plaintiff Anamari Laurentz

17. Plaintiff Anamari Laurentz is an adult individual who at all relevant times has been a citizen and resident of Suffolk County, New York.

18. Plaintiff is a former patient of Defendant and received DMES from Defendant prior to the Data Breach.

19. Plaintiff provided her Private Information to Defendant as a condition of and in exchange for obtaining DMES and related services from Defendant. Upon information and belief,

Plaintiff's Private Information was and continues to be stored and maintained in Defendant's network systems.

20. Plaintiff greatly values her privacy and is very careful about sharing her sensitive Private Information. Plaintiff diligently protects her Private Information and stores any documents containing Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

21. Plaintiff would not have provided her Private Information to Defendant had she known it would be kept using inadequate data security and vulnerable to a cyberattack.

22. At the time of the Data Breach Defendant retained Plaintiff's Private Information in its network systems with inadequate data security, causing Plaintiff's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

23. On or about October 18, 2024, Plaintiff received Defendant's Notice Letter informing that her Private Information was accessed and exposed to unauthorized hackers in the Data Breach. According to the Notice Letter, the hackers acquired files containing Plaintiff's sensitive Private Information, including her date of birth, patient number, and medical diagnosis and treatment information.

24. Plaintiff has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff now monitors her financial and credit statements multiple times a week and has spent hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities.

25. Plaintiff further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach,

Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

26. The risk of identity theft is impending and has materialized, as there is evidence that Plaintiff's and Class Members' Private Information was targeted, accessed, and misused, including through publication and dissemination on the dark web.

27. Plaintiff further believes her Private Information, and that of Class Members, was and will be sold and disseminated on the dark web following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

28. The Data Breach has also caused Plaintiff to suffer fear, anxiety, and stress about her Private Information now being in the hands of cybercriminals, which has been compounded by the fact that Defendant still has not fully informed her of key details about the Data Breach's occurrence or the information stolen.

29. Moreover, since the Data Breach Plaintiff has experienced suspicious spam calls and texts using her Private Information compromised in the Data Breach, and believes this to be an attempt to secure additional information from or about her.

Defendant Advanced Recovery Equipment and Supplies, LLC

30. Defendant Advanced Recovery Equipment and Supplies, LLC is a healthcare provider organized under New York law and with its principal place of business at 1100 Coney Island Avenue, Brooklyn, New York 11230.

JURISDICTION AND VENUE

31. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). There are at least 100 putative Class Members, the aggregated claims of the individual Class Members exceed the sum or value of \$5,000,000

exclusive of interest and costs, and members of the proposed Class are citizens of states different from Defendant, as the Data Breach affected Class Members in multiple states.

32. This Court has personal jurisdiction over Defendant because Defendant is incorporated and headquartered in New York and engaged in substantial activity in this state.

33. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) through (d) because Defendant's principal place of business is located in this District and a substantial part of the events and omissions giving rise to this action occurred in this District.

FACTUAL BACKGROUND

A. Defendant Owed Duties to Adopt Reasonable Data Security Measures for Private Information it Collected and Maintained.

34. Defendant is a healthcare provider that furnishes DMES, including bracing, continuous passive motion and cold therapy unit machines, and home care kits to patients across the Tri-State Area and other states.³

35. Plaintiff and Class Members are current and former patients of Defendant who received DMES and related healthcare services from Defendant in or prior to July 2023.

36. As a condition and in exchange for receiving healthcare services from Defendant, Defendants' patients, including Plaintiff and Class Members, were required to entrust Defendant with highly sensitive Private Information, including their names, street addresses, email addresses and/or phone number(s), Social Security numbers, dates of birth, driver's license or state-issued identification numbers, credit or debit card numbers or information, usernames and passwords associated with online accounts, health insurance policy information, medical diagnosis and treatment information, and other sensitive data.

³ See *About Us*, Advanced Recovery Equipment & Supplies, <https://advancedrecoveryequipment.com/about-us/> (last visited Nov. 4, 2024).

37. In exchange for receiving Plaintiff's and Class Members' Private Information, Defendant promised to safeguard the sensitive, confidential data and use it only for authorized and legitimate purposes, and to delete such information from its systems once there was no longer a need to maintain it.

38. The information Defendant held in its computer networks at the time of the Data Breach included the unencrypted Private Information of Plaintiff and Class Members.

39. At all relevant times, Defendant knew it was storing and using its networks to store and transmit valuable, sensitive Private Information belonging to Plaintiff and Class Members, and that as a result, its systems would be attractive targets for cybercriminals.

40. Defendant also knew that any breach of its information technology network and exposure of the data stored therein would result in the increased risk of identity theft and fraud for the individuals whose Private Information was compromised, as well as intrusion into those individuals' highly private medical information.

41. Upon information and belief, Defendant made promises and representations to its patients, including Plaintiff and Class Members, that the Private Information collected from them as a condition of obtaining healthcare services from Defendant would be kept safe and confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it were no longer required to maintain it.

42. Plaintiff and Class Members relied on these promises from Defendant, a sophisticated business entity and healthcare provider, to implement reasonable practices to keep their sensitive Private Information confidential and securely maintained, to use this information for necessary purposes only and make only authorized disclosures of this information, and to delete

Private Information from Defendant's systems when no longer necessary for its legitimate business or healthcare purposes.

43. But for Defendant's promises to keep Plaintiff's and Class Members' Private Information secure and confidential, Plaintiff and Class Members would not have sought services from or entrusted their Private Information to Defendant. Healthcare patients and consumers, in general, demand security to safeguard their Private Information, especially when sensitive medical information is involved.

44. Based on the foregoing representations and warranties and to obtain DMES and related services from Defendant, Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its promises and obligations to keep such information confidential and protected against unauthorized access.

45. Plaintiff and Class Members value the confidentiality of their Private Information and demand security to safeguard their Private Information. To that end, Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

46. Defendant derived economic benefits from collecting Plaintiff's and Class Members' Private Information. Without the required submission of Private Information, Defendant could not perform its operations, furnish the services it provides, or receive payment for those services.

47. By obtaining, using, and benefiting from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting that Private Information from unauthorized access and disclosure.

48. Defendant had and has a duty to adopt reasonable measures to keep Plaintiff's and Class Members' Private Information confidential and protected from involuntary disclosure to third parties, and to audit, monitor, and verify the integrity of its IT networks and those of its vendors and affiliates.

49. Additionally, Defendant had and has obligations created by the Federal Trade Commission ("FTC") Act, 15 U.S.C. § 45 ("FTC Act"), the Health Insurance Portability and Accountability Act ("HIPAA"), common law, contract, industry standards, and representations made to Plaintiff and Class Members, to keep their Private Information confidential and protected from unauthorized disclosure. Defendant failed to do so.

B. Defendant Failed to Adequately Safeguard Plaintiff's and Class Member's Private Information, resulting in the Data Breach.

50. On or about October 18, 2024, Defendant began sending Plaintiff and other Data Breach victims letters informing them of the Data Breach ("Notice Letters").⁴

51. The Notice Letters generally inform as follows, in part:

What Happened?

We discovered unauthorized access to our network occurred between June 27 and July 28, 2023.

What We Are Doing.

We immediately launched an investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations to analyze the extent of any compromise of the information on our network.

What Information Was Involved?

Based on our comprehensive investigation and document review, which concluded on September 29, 2024, we discovered that a

⁴ See *Advanced Recovery Equipment and Supplies, LLC Notifies Affected Individuals of Information Security Incident*, Advanced Recovery Equipment & Supplies, available at <https://advancedrecoveryequipment.com/wp-content/uploads/2024/10/Advanced-Recovery-Equipment-Supplies-LLC-Notifies-Affected-Individuals-of-Information-Security-Incident33012298.1.pdf> (last visited Nov. 4, 2024).

limited amount of personal information was removed from our network in connection with this incident, including full names and one or more of the following: Social Security numbers, dates of birth, driver's license numbers or state identification numbers, credit or debit card information, usernames and passwords associated with one (1) or more online accounts, medical information, and/or health insurance policy information.

52. Omitted from the Notice Letter were the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their Private Information is protected.

53. Thus, Defendant's purported 'disclosure' amounts to no real disclosure at all, as it fails to inform Plaintiff and Class Members of the Data Breach's critical facts with any degree of specificity. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

54. To make matters worse, although the Data Breach's occurred from June–July, 2023, Defendant purportedly did not discover it until September 29, 2024, and waited an additional month after that before notifying the public or affected individuals of the Data Breach, diminishing Plaintiff's and Class Members' ability to timely and thoroughly mitigate and address harms resulting from their Private Information's unauthorized disclosure.

55. Plaintiff's and Class Members' Private Information was targeted, accessed, and stolen by cybercriminals in the Data Breach. Criminal hackers accessed and acquired confidential files containing Plaintiff's and Class Members' Private Information from Defendant's network systems, where they were kept without adequate safeguards and in unencrypted form.

56. Defendant could have prevented this Data Breach by properly training personnel and/or securing and encrypting the files and file servers containing Plaintiff's and Class Members' Private Information, but failed to do so.

57. As the Data Breach evidences, Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive Private Information it collected and maintained from Plaintiff and Class Members, such as standard monitoring and altering techniques, encrypting the information, or deleting the information when it is no longer needed. These failures by Defendant allowed and caused cybercriminals to target Defendant's network, carry out the Data Breach for a month without detection, and exfiltrate files containing Plaintiff and Class Member's Private Information.

58. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing Plaintiff's and Class Members' Private Information, using controls like limitations on personnel with access to sensitive data and requiring multi-factor authentication ("MFA") for access, training its employees on standard cybersecurity practices, and implementing reasonable logging and alerting methods to detect unauthorized access.

59. For example, if Defendant had implemented industry standard logging, monitoring, and alerting systems—basic technical safeguards that any PHI and/or PII-collecting company is expected to employ—then cybercriminals would not have been able to perpetrate prolonged malicious activity in Defendant's network systems for over a month without alarm bells going off, including the reconnaissance necessary to identify where Defendant stored Private Information, installation of malware or other methods of establishing persistence and creating a path to exfiltrate data, staging data in preparation for exfiltration, and then exfiltrating that data outside of Defendant's system without being caught.

60. Defendant would have recognized the malicious activities detailed in the preceding paragraph if it bothered to implement basic monitoring and detection systems, which then would have stopped the Data Breach or greatly reduced its impact.

61. Defendant's tortious conduct and breach of contractual obligations, as detailed herein, are evidenced by its failure to recognize the Data Breach until cybercriminals had already accessed Plaintiff's and Class Members' Private Information, meaning Defendant had no effective means in place to ensure that cyberattacks were detected and prevented.

C. Defendant Knew of the Risk of a Cyberattack because Healthcare Providers in Possession of Private Information are Particularly Susceptable.

62. Defendant's negligence in failing to safeguard Plaintiff's and Class Members' Private Information is exacerbated by the repeated warnings and alerts directed to protecting and securing such data.

63. Private Information of the kind accessed in the Data Breach is of great value to hackers and cybercriminals as it can be used for a variety of unlawful and nefarious purposes, including ransomware, fraudulent misuse, and sale on the Dark web.

64. Private Information can also be used to distinguish, identify, or trace an individual's identity, such as their name, Social Security number, and financial records. This may be accomplished alone, or in combination with other personal or identifying information that is connected, or linked to an individual, such as his or her birthdate, birthplace, and mother's maiden name.

65. Data thieves regularly target entities in the healthcare industry like Defendant due to the highly sensitive information that such entities maintain. Defendant knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

66. Cyber-attacks against institutions such as Defendant are targeted and frequent. According to Contrast Security's 2023 report *Cyber Bank Heists: Threats to the financial sector*, "Over the past year, attacks have included banking trojans, ransomware, account takeover, theft of client data and cybercrime cartels deploying 'trojanized' finance apps to deliver malware in spear-phishing campaigns."⁵ In fact, "40% [of financial institutions] have been victimized by a ransomware attack."⁶

67. In light of past high profile data breaches at industry-leading companies, including, for example, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or, if acting as a reasonable healthcare provider, should have known that the Private Information it collected and maintained would be vulnerable to and targeted by cybercriminals.

68. According to the Identity Theft Resource Center's report covering the year 2021, "the overall number of data compromises (1,862) is up more than 68 percent compared to 2020. The new record number of data compromises is 23 percent over the previous all-time high (1,506) set in 2017. The number of data events that involved sensitive information (Ex: Social Security numbers) increased slightly compared to 2020 (83 percent vs. 80 percent)."⁷

⁵ Contrast Security, "Cyber Bank Heists: Threats to the financial sector," pg. 5, avail. at <https://www.contrastsecurity.com/hubfs/Cyber%20Bank%20Heists%20Report%2023.pdf?hsLang=en> (last acc. February 9, 2024).

⁶ *Id.*, at 15.

⁷ See "Identity Theft Resource Center's 2021 Annual Data Breach Report Sets New Record for Number of Compromises," Jan. 24, 2022, available at <https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/> (last accesses Feb. 9, 2024).

69. The increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant itself. According to IBM's 2022 report, "[f]or 83% of companies, it's not if a data breach will happen, but when."⁸

70. Defendant's data security obligations were particularly important given the substantial increase, preceding the date of the subject Data Breach, in cyberattacks and/or data breaches targeting healthcare entities like Defendant that collect and store PHI.

71. For example, of the 1,862 data breaches recorded in 2021, 330 of them, or 17.7%, were in the healthcare industry.⁹

72. The 330 breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.¹⁰

73. Entities in custody of PHI, like Defendant, reported the largest number of data breaches among all measured sectors in 2022, with the highest rate of exposure per breach.¹¹ Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found the "average total cost to resolve an identity theft-related incident . . . came to about \$20,000," and that victims were often forced to pay out of pocket costs for healthcare they did not receive in order to restore coverage.¹² Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30

⁸ IBM, "Cost of a data breach 2022: A million-dollar race to detect and respond," available at <https://www.ibm.com/reports/data-breach> (last accessed Feb. 9, 2024).

⁹ 2021 Data Breach Annual Report (ITRC, Jan. 2022), <https://notified.idtheftcenter.org/s/>, at 6.

¹⁰ *Id.*

¹¹ See Identity Theft Resource Center, 2022 Annual Data Breach Report, <https://www.idtheftcenter.org/publication/2022-data-breach-report/> (last accessed May 8, 2024).

¹² See Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), <https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/> (last accessed May 8, 2024).

percent said their insurance premiums went up after the event. 40 percent of the patients were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals, and detrimentally impact the economy as a whole.¹³

74. Thus, the healthcare industry has become a prime target for threat actors: “High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks.”¹⁴

75. As indicated by Jim Trainor, second in command at the FBI’s cyber security division: “Medical records are a gold mine for criminals—they can access a patient’s name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI records can go from \$20 say up to—we’ve even seen \$60 or \$70.”¹⁵ A complete identity theft kit with health insurance credentials may be worth up to \$1,000 on the black market, whereas stolen payment card information sells for about \$1.¹⁶

76. As a healthcare entity in possession of its patients’ and clients’ PHI, Defendant knew, or should have known, the importance of safeguarding the PHI entrusted to it by Plaintiff and Class Members and of the foreseeable consequences if its data security systems were breached. Such consequences include the significant costs imposed on Plaintiff and Class Members due to a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

¹³ *Id.*

¹⁴ <https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/>.

¹⁵ IDEXperts, You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows: <https://www.idexperts.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat>.

¹⁶ PriceWaterhouseCoopers, *Managing cyber risks in an interconnected world*, Key findings from The Global State of Information Security® Survey 2015: <https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf>.

77. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and Class Members from being wrongfully disclosed to cybercriminals.

78. Given the nature of the Data Breach, it was foreseeable that Plaintiff's and Class Members' Private Information compromised therein would be targeted by hackers and cybercriminals for use in variety of different injurious ways. Indeed, the cybercriminals who possess Plaintiff's and Class Members' Private Information can easily obtain their tax returns or open fraudulent credit card accounts in Plaintiff's and Class Members' names.

79. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on its network server(s), amounting to hundreds of thousands of individuals' detailed Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of that unencrypted data.

80. Plaintiff and Class Members were the foreseeable and probable victims of Defendant's inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing Private Information and the critical importance of providing adequate security for that information.

81. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Plaintiff and Class Members especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and the like.

D. Defendant was Required, but Failed to Comply with FTC Rules and Guidance.

82. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

83. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses like Defendant. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.¹⁷

84. The FTC's guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.¹⁸

85. The FTC further recommends that companies not maintain confidential personal information, like Private Information, longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

86. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect third parties' confidential data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting

¹⁷ *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed May 8, 2024).

¹⁸ *Id.*

from these actions further clarify the measures business like Defendant must undertake to meet their data security obligations.

87. Such FTC enforcement actions include actions against healthcare entities like Defendant. *See, e.g., In the Matter of LabMD, Inc.*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) (“[T]he Commission concludes that LabMD’s data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.”).

88. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect sensitive personal information, like Private Information. The FTC publications and orders described above also form part of the basis of Defendant’s duty in this regard.

89. The FTC has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that “most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit.”¹⁹

90. Defendant failed to properly implement basic data security practices, in violation of its duties under the FTC Act.

91. Defendant’s failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff’s and Class Members’ Private Information or to comply

¹⁹ Statement of FTC Commissioner Pamela Jones Harbour (Remarks Before FTC Exploring Privacy Roundtable), <http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf>.

with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

E. Defendant was Required, But Failed to Comply with HIPAA Guidelines.

92. Defendant is a covered business under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E; and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and C.

93. Defendant is further subject to the Health Information Technology Act (“HITECH”)’s rules for safeguarding electronic forms of medical information. *See* 42 U.S.C. §17921; 45 C.F.R. § 160.103.

94. HIPAA’s Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting Private Information that is kept or transferred in electronic form.

95. HIPAA requires “compl[iance] with the applicable standards, implementation specifications, and requirements” of HIPAA “with respect to electronic protected health information.” 45 C.F.R. § 164.302. “Electronic protected health information” is “individually identifiable health information . . . that is (i) transmitted by electronic media; maintained in electronic media.” 45 C.F.R. § 160.103.

96. HIPAA’s Security Rule required and requires that Defendant do the following:

- a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;
- b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

- c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and
- d. Ensure compliance by its workforce.

97. HIPAA also requires Defendant to “review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information.” 45 C.F.R. § 164.306(e). Additionally, Defendant is required under HIPAA to “[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights.” 45 C.F.R. §164.312(a)(1).

98. HIPAA and HITECH also require procedures to prevent, detect, contain, and correct data security violations and disclosures of Private Information that are reasonably anticipated but not permitted by privacy rules. *See* 45 C.F.R. § 164.306(a)(1), (a)(3).

99. HIPAA further requires a covered entity like Defendant to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

100. HIPAA further requires a covered entity like Defendant to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of PHI in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

101. HIPAA also requires the Office of Civil Rights (“OCR”), within the Department of Health and Human Services (“HHS”), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, “HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule.” US Department of Health & Human Services, Security Rule Guidance Material.²⁰ The list of resources includes a link to guidelines set by the National Institute of Standards and Technology, which OCR says “represent the industry standard for good business practices with respect to standards for securing e-PHI.” US Department of Health & Human Services, Guidance on Risk Analysis.²¹

102. As alleged in this Complaint, Defendant failed to comply with HIPAA and HITECH. It failed to maintain adequate security practices, systems, and protocols to prevent data loss, failed to mitigate the risks of a data breach, and failed to ensure the confidentiality and protection of Plaintiff’s and Class Members’ Private Information, including PHI.

F. Defendant Failed to Comply with Industry Standards.

103. A number of industry and national best practices have been published and are widely used as a go-to resource when developing an institution’s cybersecurity standards.

104. The Center for Internet Security’s (CIS) Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and

²⁰ <https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html> (last accessed Feb. 13, 2024).

²¹ *Id.*

Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.²²

105. In addition, the NIST recommends certain practices to safeguard systems²³:

- a. Control who logs on to your network and uses your computers and other devices.
- b. Use security software to protect data.
- c. Encrypt sensitive data, at rest and in transit.
- d. Conduct regular backups of data.
- e. Update security software regularly, automating those updates if possible.
- f. Have formal policies for safely disposing of electronic files and old devices.
- g. Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.

106. Further still, the Cybersecurity & Infrastructure Security Agency makes specific recommendations to organizations to guard against cybersecurity attacks, including (a) reducing the likelihood of a damaging cyber intrusion by validating that “remote access to the organization’s

²² See Rapid7, “CIS Top 18 Critical Security Controls Solutions,” available at <https://www.rapid7.com/solutions/compliance/critical-controls/> (last acc. Feb. 9, 2024).

²³ Federal Trade Commission, “Understanding The NIST Cybersecurity Framework,” <https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework> (last acc. Feb. 9, 2024).

network and privileged or administrative access requires multi-factor authentication, [e]nsur[ing] that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA[,] [c]onfirm[ing] that the organization’s IT personnel have disabled all ports and protocols that are not essential for business purposes,” and other steps; (b) taking steps to quickly detect a potential intrusion, including “[e]nsur[ing] that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior [and] [e]nabl[ing] logging in order to better investigate issues or events[;] [c]onfirm[ing] that the organization’s entire network is protected by antivirus/antimalware software and that signatures in these tools are updated,” and (c) “[e]nsur[ing] that the organization is prepared to respond if an intrusion occurs,” and other steps.²⁴

107. Upon information and belief, Defendant failed to implement industry-standard cybersecurity measures, including by failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security’s Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, and by failing to comply with other industry standards for protecting Plaintiff’s and Class Members’ Private Information, resulting in the Data Breach.

G. Defendant Owed Plaintiff and Class Members a Common Law Duty to Safeguard their Private Information.

108. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing,

²⁴ Cybersecurity & Infrastructure Security Agency, “Shields Up: Guidance for Organizations,” available at <https://www.cisa.gov/shields-guidance-organizations> (last acc. Feb. 9, 2024).

safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant's duty owed to Plaintiff and Class Members obligated it to provide reasonable data security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected Plaintiff's and Class Members' Private Information.

109. Defendant owed a duty to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect the Private Information in its possession, including adequately training its employees and others who accessed Private Information within its computer systems on how to adequately protect Private Information.

110. Defendant owed a duty to Plaintiff and Class Members to implement processes that would detect a compromise of Private Information in a timely manner and act upon data security warnings and alerts in a timely fashion.

111. Defendant owed a duty to Plaintiff and Class Members to disclose in a timely and accurate manner when and how the Data Breach occurred.

112. Defendant owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

113. Defendant failed to take the necessary precautions required to safeguard and protect Plaintiff's and Class Members' Private Information from unauthorized disclosure. Defendant's actions and omissions represent a flagrant disregard of Plaintiff's and Class Members' rights.

H. Plaintiff and Class Members Suffered Common Injuries and Damages due to Defendant's conduct.

114. Defendant's failure to implement or maintain adequate data security measures for Plaintiff's and Class Members' Private Information directly and proximately injured Plaintiff and Class Members by the resulting disclosure of their Private Information in the Data Breach.

115. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiff and Class Members are long lasting and severe. Once Private Information is stolen fraudulent use of that information and damage to victims may continue for years.

116. Plaintiff and Class Members are also at a continued risk because their Private remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack and are subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect its patients' = Private Information.

117. As a result of Defendant's ineffective and inadequate data security practices, the resulting Data Breach, and the foreseeable consequences of their Private Information ending up in criminals' possession, the risk of identity theft to Plaintiff and Class Members has materialized and is imminent, and they have all sustained actual injuries and damages, including, without limitation, (a) invasion of privacy; (b) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (d) financial costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) deprivation of value of their Private Information; (g) loss of the benefit of their bargain with Defendant; (h) emotional distress including anxiety and stress in dealing with the Data Breach's aftermath; and (i) the continued risk to their sensitive Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information it collects and maintains.

The Risk of Identity Theft to Plaintiff and Class Members is Present and Ongoing

118. Plaintiff and Class Members are at a heightened risk of identity theft for years to come because of the Data Breach.

119. The FTC defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.”²⁵ The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including “[n]ame, Social Security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.”²⁶

120. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal individuals’ personal data to monetize the information. Criminals monetize the data by selling the stolen information on the internet black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

121. The dark web is an unindexed layer of the internet that requires special software or authentication to access.²⁷ Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or “surface” web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA’s web address is cia.gov, but on the dark web the CIA’s web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.²⁸ This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

122. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, personal and medical information like the Private

²⁵ 17 C.F.R. § 248.201 (2013).

²⁶ *Id.*

²⁷ *What Is the Dark Web?*, Experian, available at <https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/>.

²⁸ *Id.*

Information at issue here.²⁹ The digital character of Private Information stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of birth, and medical information.³⁰ As Microsoft warns “[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others.”³¹

123. The unencrypted Private Information of Plaintiff and Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted and detailed Private Information may fall into the hands of companies that will use it for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the Plaintiff’s and Class Members’ Private Information.

124. Because a person’s identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim’s identity, or to track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

125. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as “social engineering” to obtain even more information about a

²⁹ *What is the Dark Web?* – Microsoft 365, available at <https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web>.

³⁰ *Id.*; *What Is the Dark Web?*, Experian, available at <https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/>.

³¹ *What is the Dark Web?* – Microsoft 365, available at <https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web>.

victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

126. Identity thieves can also use an individual's personal data and Private Information to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's information, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant issued in the victim's name.³²

127. Theft of PHI, in particular, is gravely serious: "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."³³

128. Health information is likely to be used in detrimental ways, including by leveraging sensitive personal health details and diagnoses to extort or coerce someone, and serious and long-term identity theft.³⁴

³² *Identity Theft and Your Social Security Number*, Social Security Administration, 1 (2018), <https://www.ssa.gov/pubs/EN-05-10064.pdf>.

³³ See Federal Trade Commission, Medical Identity Theft, <http://www.consumer.ftc.gov/articles/0171-medical-identity-theft>.

³⁴ *Id.*

129. Another study found “the majority [70%] of data impacted by healthcare breaches could be leveraged by hackers to commit fraud or identity theft.”³⁵

130. “Actors buying and selling PII and PHI from healthcare institutions and providers in underground marketplaces is very common and will almost certainly remain so due to this data’s utility in a wide variety of malicious activity ranging from identity theft and financial fraud to crafting of bespoke phishing lures.”³⁶

131. “Medical identity theft is a great concern not only because of its rapid growth rate, but because it is the most expensive and time consuming to resolve of all types of identity theft. Additionally, medical identity theft is very difficult to detect which makes this form of fraud extremely dangerous.”³⁷

132. The reality is that cybercriminals seek nefarious outcomes from a data breach” and “stolen health data can be used to carry out a variety of crimes.”³⁸

133. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of “Fullz” packages.³⁹

³⁵<https://healthissecurity.com/news/70-of-data-involved-in-healthcare-breaches-increases-risk-of-fraud>.

³⁶ *Id.*

³⁷ <https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf>.

³⁸ <https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon>.

³⁹ “Fullz” is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even “dead Fullz,” which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a “mule account” (an account that will accept a fraudulent money transfer from a compromised account) without the victim’s knowledge. *See, e.g.,* Brian Krebs, *Medical Records for Sale in Underground*

134. With “Fullz” packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals.

135. The development of “Fullz” packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff’s and Class Members’ phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

136. Thus, even if certain information (such as driver’s license numbers) was not stolen in the data breach, criminals can still easily create a comprehensive “Fullz” package.

137. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

138. The development of “Fullz” packages means that stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff’s and Class Members’ phone numbers, email addresses, and other unregulated sources and identifiers. That is exactly what is happening to Plaintiff and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that their stolen Private Information is being misused, and that such misuse is traceable to the Data Breach.

Stolen from Texas Life Insurance Firm, Krebs on Security (Sep. 18, 2014), <https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm> (last visited Feb. 26, 2024).

139. Victims of identity theft can suffer from both direct and indirect financial losses.

According to a research study published by the Department of Justice:

A direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss.^[40]

140. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than \$3.5 billion in losses to individuals and business victims.⁴¹

141. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."⁴² Yet, Defendant failed to rapidly report to Plaintiff and the Class that their Private Information was stolen.

142. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

143. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their Private Information. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously

⁴⁰ Erika Harrell, *Bureau of Just. Stat.*, U.S. DEP'T OF JUST., NCJ 256085, *Victims of Identity Theft*, 2018 I (2020) <https://bjs.ojp.gov/content/pub/pdf/vit18.pdf> (last accessed Jan. 23, 2024).

⁴¹ See <https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120>.

⁴² *Id.*

monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

144. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen Private Information. To protect themselves, Plaintiff and Class Members will need to remain vigilant for years or even decades to come.

Loss of Time to Mitigate the Risk of Identify Theft and Fraud

145. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet the asset of time has been lost.

146. In the event that Plaintiff and Class Members experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record

147. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must monitor their financial accounts for many years to mitigate that harm.

148. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing “freezes” and “alerts” with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover.

149. These efforts are consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.⁴³

150. Once Private Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of Defendant's conduct that caused the Data Breach.

Diminished Value of Private Information

151. Personal data like Private Information is a valuable property right.⁴⁴ Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

152. For example, drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PHI on the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach

⁴³ See Federal Trade Commission, *Identity Theft.gov*, <https://www.identitytheft.gov/Steps> (last visited Feb. 26, 2024).

⁴⁴ See, e.g., John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PRIVATE INFORMATION") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PRIVATE INFORMATION, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

153. Medical information is especially valuable to identity thieves. According to account monitoring company LogDog, medical data sells on the dark web for \$50 and up.⁴⁵

154. An active and robust legitimate marketplace for personal information also exists. In 2019, the data brokering industry was worth roughly \$200 billion.⁴⁶ In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.^{47, 48} Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to \$50 a year.⁴⁹

155. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and black markets, has been damaged and diminished in its value by its unauthorized and likely release onto the dark web, where holds significant value for the threat actors.

156. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

⁴⁵ <https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content>.

⁴⁶ <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>.

⁴⁷ <https://datacoup.com/>.

⁴⁸ <https://digi.me/what-is-digime/>.

⁴⁹ Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at <https://computermobilepanel.nielsen.com/ui/US/en/faen.html>.

Future Cost of Credit and Identify Theft Monitoring is Reasonable and Necessary

157. To date, Defendant has done little to provide Plaintiff and Class Members with relief for the damages they have suffered as a result of the Data Breach.

158. Given the type of targeted attack in this case and sophisticated criminal activity, the type of information involved, and the *modus operandi* of cybercriminals, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes—*e.g.*, opening bank accounts in the victims’ names to make purchases or to launder money; filing false tax returns; taking out loans or insurance; or filing false unemployment claims.

159. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her information was used to file for unemployment benefits until law enforcement notifies the individual’s employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual’s authentic tax return is rejected.

160. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.⁵⁰ The information disclosed in this Data Breach is impossible to “close” and difficult, if not impossible, to change (such as medical histories).

161. Consequently, Plaintiff and Class Members are at a present and ongoing risk of fraud and identity theft for many years into the future.

⁵⁰ See Jesse Damiani, *Your Social Security Number Costs \$4 On The Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), <https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1>.

162. The retail cost of credit monitoring and identity theft monitoring can cost \$200 or more a year per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their Private Information.

Loss of Benefit of the Bargain

163. Furthermore, Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain.

164. When agreeing to provide their Private Information, which was a condition precedent to obtain services from Defendant, and paying Defendant, directly or indirectly, for its services, Plaintiff and Class Members, as patients and consumers, understood and expected that they were, in part, paying for services and data security to protect the Private Information they were required to provide.

165. In fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains struck with Defendant.

CLASS REPRESENTATION ALLEGATIONS

166. Plaintiff brings this nationwide class action individually and on behalf of all other persons similarly situated pursuant to Federal Rule of Civil Procedure 23(a) and 23(b).

167. Plaintiff proposes the following nationwide class definition, subject to amendment as appropriate:

All individuals residing in the United States whose Private Information may have been compromised in the Data Breach, including all individuals who received a Notice Letter (the "Class").

168. Excluded from the Class are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

169. Plaintiff hereby reserves the right to amend or modify the Class definition with greater specificity or division after having had an opportunity to conduct discovery.

170. Numerosity. The members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief including Defendant's reporting, the Class consists at 156,000 individuals whose Private Information was compromised in Data Breach.

171. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

- a. Whether Defendant unlawfully used, maintained, lost, or disclosed Class Members' Private Information;
- b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

- e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;
- f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;
- g. Whether computer hackers obtained Class Members' Private Information in the Data Breach;
- h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;
- i. Whether Class Members suffered legally cognizable damages as a result of Defendant's misconduct;
- j. Whether Defendant's conduct was negligent;
- k. Whether Defendant breached implied contracts for adequate data security with Class Members;
- l. Whether Defendant was unjustly enriched by retention of the monetary benefits conferred on it by Class Members; and
- m. Whether Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

172. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach.

173. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

174. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' Private Information was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

175. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial and party resources, and protects the rights of each Class Member.

176. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and declaratory relief are appropriate on a class-wide basis.

177. Likewise, particular issues are appropriate for certification pursuant to Federal Rule of Civil Procedure 23(c)(4) because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to the following:

- a. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

- b. Whether Defendant's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;
- c. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;
- d. Whether Defendant failed to take commercially reasonable steps to safeguard patient Private Information; and
- e. Whether adherence to FTC and HIPAA data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

178. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified by Defendant.

CAUSES OF ACTION

COUNT I NEGLIGENCE/NEGLIGENCE *PER SE* (On Behalf of Plaintiff and the Class)

179. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 178 above as if fully set forth herein.

180. Defendant required Plaintiff and Class Members to submit sensitive, confidential Private Information to Defendant as a condition of receiving healthcare services from Defendant.

181. Plaintiff and Class Members provided their Private Information to Defendant, including their names, Social Security numbers, dates of birth, health insurance information, medical diagnosis and treatment information, and other sensitive data.

182. Defendant had full knowledge of the sensitivity of the Private Information to which it was entrusted, and the types of harm that Plaintiff and Class Members could and would suffer if the Private Information was wrongfully disclosed to unauthorized persons.

183. Defendant owed a duty to Plaintiff and each Class Member to exercise reasonable care in holding, safeguarding, and protecting the Private Information it collected from them.

184. Plaintiff and Class Members were the foreseeable victims of any inadequate data safety and security practices by Defendant.

185. Plaintiff and the Class Members had no ability to protect their Private Information in Defendant's possession.

186. By collecting, transmitting, and storing Plaintiff's and Class Members' Private Information Defendant owed Plaintiff and Class Members a duty of care to use reasonable means to secure and safeguard their Private Information, to prevent the information's unauthorized disclosure, and to safeguard it from theft or exfiltration to cybercriminals. Defendant's duty included the responsibility to implement processes by which it could detect and identify malicious activity or unauthorized access on its networks or servers.

187. Defendant owed a duty of care to Plaintiff and the Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that controls for its networks, servers, and systems, and the personnel responsible for them, adequately protected Plaintiff's and Class Members' Private Information.

188. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between it and its patients, which is recognized by laws and regulations including but not limited to the FTC Act and HIPAA, as well as the common law. Defendant was

able to ensure its network servers and systems were sufficiently protected against the foreseeable harm a data breach would cause Plaintiff and Class Members, yet it failed to do so.

189. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

190. Pursuant to the FTC Act, 15 U.S.C. § 45 *et seq.*, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff’s and Class Members’ Private Information.

191. Pursuant to HIPAA, 42 U.S.C. § 1302d *et seq.*, Defendant had the further duty to implement reasonable safeguards to protect Plaintiffs’ and Class Members’ PHI from unauthorized disclosure.

192. Pursuant to HIPAA, Defendant had a duty to implement reasonable data security measures for the PHI in its care, including by, *e.g.*, rendering the electronic PHI in a form unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.” *See* 45 C.F.R. § 164.304.

193. Additionally, pursuant to HIPAA, Defendant had a duty to provide notice of the Data Breach within 60 days of discovering it. *See* 42 C.F.R. § 2.16(b); 45 C.F.R. § 164.404(b).

194. Defendant breached its duties to Plaintiff and Class Members under the FTC Act and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices and procedures to safeguard Plaintiff’s and Class Members’ Private Information, by

failing to ensure the Private Information in its systems was encrypted and timely deleted when no longer needed, and by failing to provide notice to Plaintiffs and Class Members of the Data Breach until over 60 days after discovering it.

195. The injuries to Plaintiff and Class Members resulting from the Data Breach were directly and indirectly caused by Defendant's violations of the FTC Act and HIPAA.

196. Plaintiff and Class Members are within the class of persons the FTC Act, HIPAA, and Part 2 are intended to protect.

197. The type of harm that resulted from the Data Breach was the type of harm the FTC Act and HIPAA are intended to guard against.

198. Defendant's failures to comply with the FTC Act or HIPAA constitute negligence *per se*.

199. Defendant's duty to use reasonable care in protecting Plaintiff's and Class Members' confidential Private Information in its possession arose not only because of the statutes and regulations described above, but also because Defendant is bound by industry standards to reasonably protect such Private Information.

200. Defendant breached its duties of care, and was grossly negligent, by acts of omission or commission, including by failing to use reasonable measures or even minimally reasonable measures to protect the Plaintiff's and Class Members' Private Information from unauthorized disclosure in this Data Breach.

201. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and Class Members' Private Information;

- b. Maintaining and/or transmitting Plaintiff's and Class Members' Private Information in unencrypted and identifiable form;
- c. Failing to implement data security measures, like adequate MFA for as many systems as possible, to safeguard against known techniques for initial unauthorized access to network servers and systems;
- d. Failing to adequately train employees on proper cybersecurity protocols;
- e. Failing to adequately monitor the security of its networks and systems;
- f. Failure to periodically ensure its network system had plans in place to maintain reasonable data security safeguards;
- g. Allowing unauthorized access to Plaintiff's and Class Members' Private Information; and
- h. Failing to adequately notify Plaintiff and Class Members about the Data Breach so they could take appropriate steps to mitigate damages.

202. But for Defendant's wrongful and negligent breaches of its duties owed to Plaintiff and Class Members, their Private Information would not have been compromised because the malicious activity would have been identified and stopped before criminal hackers had a chance to inventory Defendant's digital assets, stage them, and then exfiltrate them.

203. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiff's and Class Members' Private Information would injure Plaintiff and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in Defendant's industry.

204. It was therefore foreseeable that the failure to adequately safeguard Plaintiff's and Class Members' Private Information would cause them one or more types of injuries.

205. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer injuries, including but not limited to (a) invasion of privacy; (b) lost or diminished value of their Private Information; (c) actual identity theft, or the imminent and substantial risk of identity theft or fraud; (d) out-of-pocket and lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (e) loss of benefit of the bargain; (f) anxiety and emotional harm due to their Private Information's disclosure to cybercriminals; and (g) the continued and certainly increased risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect it.

206. Plaintiff and Class Members are entitled to damages, including compensatory, consequential, punitive, and nominal damages, in an amount to be proven at trial.

207. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (a) strengthen its data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) provide adequate and lifetime credit monitoring to Plaintiff and all Class Members.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

208. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 178 above as if fully set forth herein.

209. Defendant required Plaintiff and Class Members to provide and entrust their Private Information to Defendant as a condition of and in exchange for receiving healthcare services from Defendant.

210. When Plaintiff and Class Members provided their Private Information to Defendant, they entered into implied contracts with Defendant pursuant to which Defendant agreed to safeguard and protect such Private Information and to timely and accurately notify Plaintiff and Class Members if and when their Private Information was breached and compromised.

211. Specifically, Plaintiff and Class Members entered into valid and enforceable implied contracts with Defendant when they agreed to provide their Private Information to Defendant, and Defendant agreed to reasonably protect it.

212. The valid and enforceable implied contracts that Plaintiff and Class Members entered into with Defendant included Defendant's promises to protect Private Information it collected from Plaintiff and Class Members, or created on its own, from unauthorized disclosures. Plaintiff and Class Members provided this Private Information in reliance on Defendant's promises.

213. Under the implied contracts, Defendant promised and was obligated to (a) provide healthcare services to Plaintiff and Class Members; and (b) protect Plaintiff's and Class Members' Private Information provided to obtain such services and/or created in connection therewith. In exchange, Plaintiff and Class Members agreed to provide Defendant with payment and their Private Information.

214. Defendant promised and warranted to Plaintiff and Class Members to maintain the privacy and confidentiality of the Private Information it collected from Plaintiff and Class Members and to keep such information safeguarded against unauthorized access and disclosure.

215. Defendant's adequate protection of Plaintiff's and Class Members' Private Information was a material aspect of these implied contracts with Defendant.

216. Defendant solicited and invited Plaintiff and Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

217. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with industry standards and relevant laws and regulations, including the FTC Act and HIPAA, as well as industry standards.

218. Plaintiff and Class Members who contracted with Defendant for healthcare services including reasonable data protection and provided their Private Information to Defendant reasonably believed and expected that Defendant would adequately employ adequate data security to protect that Private Information.

219. A meeting of the minds occurred when Plaintiff and Class Members agreed to, and did, provide their Private Information to Defendant and agreed Defendant would receive payment for, amongst other things, the protection of their Private Information.

220. Plaintiff and Class Members performed their obligations under the contracts when they provided their Private Information and/or payment to Defendant.

221. Defendant materially breached its contractual obligations to protect the Private Information it required Plaintiff and Class Members to provide when that Private Information was unauthorizedly disclosed in the Data Breach due to Defendant's inadequate data security measures and procedures.

222. Defendant materially breached its contractual obligations to deal in good faith with Plaintiff and Class Members when it failed to take adequate precautions to prevent the Data Breach and failed to promptly notify Plaintiff and Class Members of the Data Breach.

223. Defendant materially breached the terms of its implied contracts, including but not limited to by failing to comply with industry standards or the standards of conduct embodied in statutes or regulations like Section 5 of the FTC Act and HIPAA, and by failing to otherwise protect Plaintiff's and Class Members' Private Information, as set forth *supra*.

224. The Data Breach was a reasonably foreseeable consequence of Defendant's breaches of these implied contracts with Plaintiff and Class Members.

225. As a result of Defendant's failures to fulfill the data security protections promised in these contracts, Plaintiff and Class Members did not receive the full benefit of their bargains with Defendant, and instead received services of a diminished value compared to that described in the implied contracts. Plaintiff and Class Members were therefore damaged in an amount at least equal to the difference in the value of the services with data security protection they paid for and that which they received.

226. Had Defendant disclosed that its data security procedures were inadequate or that it did not adhere to industry standards for cybersecurity, neither Plaintiffs, Class Members, nor any reasonable person would have contracted with Defendant.

227. Plaintiff and Class Members would not have provided and entrusted their Private Information to Defendant in the absence of the implied contracts between them and Defendant.

228. Defendant breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect their Private Information and by failing to provide timely or adequate notice that their Private Information was compromised in and due to the Data Breach.

229. As a direct and proximate result of Defendant's breach of its implied contracts with Plaintiff and Class Members and the attendant Data Breach, Plaintiff and Class Members have

suffered injuries and damages as set forth herein and have been irreparably harmed, as well as suffering and the loss of the benefit of the bargain they struck with Defendant.

230. Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT III: INVASION OF PRIVACY/INTRUSION UPON SECLUSION
(On behalf of Plaintiff and the Class)

231. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 178 above as if fully set forth herein.

232. Plaintiff and Class Members had a legitimate expectation of privacy to their Private Information and were entitled to Defendant's protection of this Private Information in its possession against disclosure to unauthorized third parties.

233. Defendant owed a duty to its patients, including Plaintiff and Class Members, to keep their Private Information confidential and secure.

234. Defendant failed to protect Plaintiff's and Class Members' Private Information and instead exposed it to unauthorized persons, a criminal ransomware group, which on information and belief has made or imminently will make the Private Information publicly available and disseminated it to thousands of people, including through publishing the data on dark web leak sites, where cybercriminals go to find their next identity theft and extortion victims.

235. Defendant allowed unauthorized third parties access to and examination of the Private Information of Plaintiff and Class Members, by way of Defendant's failure to protect the Private Information through reasonable data security measures.

236. The unauthorized release to, custody of, and examination by unauthorized third parties of the Private Information of Plaintiff and Class Members is highly offensive to a

reasonable person and represents an intrusion upon Plaintiff's and Class Members' seclusion as well as a public disclosure of private facts.

237. The intrusion was into a place or thing, which was private and is entitled to be private—sensitive and confidential information including private medical histories, diagnoses, and prescriptions.

238. Plaintiff and Class Members disclosed their Private Information to Defendant as a condition of and in exchange for receiving DMES and related healthcare services, but privately with an intention that the Private Information would be kept confidential and protected from unauthorized disclosure. Plaintiff and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization, given Defendant's promises to that effect.

239. Subsequent to the intrusion, Defendant permitted Plaintiff's and Class Members' data to be published online to countless cybercriminals whose mission is to misuse such information, including through identity theft and extortion.

240. The Data Breach constitutes an intentional or reckless interference by Defendant with Plaintiff's and Class Members' interests in solitude or seclusion, as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person—including but not limited to private and personal medical diagnosis and treatment information.

241. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur, because it had actual knowledge that its information security practices were inadequate and insufficient to protect Plaintiff's and Class Members' Private Information from unauthorized disclosure.

242. Defendant acted with reckless disregard for Plaintiff's and Class Members' privacy when it allowed improper access to its systems containing Plaintiff's and Class Members' Private Information without protecting said data from the unauthorized disclosure, or even encrypting such information.

243. Defendant was aware of the potential of a data breach and failed to adequately safeguard its network systems or implement appropriate policies to prevent the unauthorized release of Plaintiff's and Class Members' Private Information to cybercriminals.

244. Because Defendant acted with this knowing state of mind, it had notice and knew that its inadequate and insufficient information security practices would cause injury and harm to Plaintiff and Class Members.

245. As a direct and proximate result of Defendant's acts and omissions set forth above, Plaintiff's and Class Members' Private Information was disclosed to third parties without authorization, causing Plaintiff and Class Members to suffer injuries and damages including, without limitation, (a) invasion of privacy; (b) lost or diminished value of their Private Information; (c) out-of-pocket and lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (d) emotional distress due to their Private Information's publication on the dark web; and (e) the continued and certainly increased risk to their Private Information, which remains in Defendant's possession in unencrypted form and subject to further unauthorized disclosures, so long as Defendant fails to undertake appropriate and adequate measures to protect it.

246. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that the Private Information maintained by Defendant can be viewed, distributed, and

used by unauthorized persons for years to come. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and Class Members.

COUNT IV
BREACH OF CONFIDENCE
(On Behalf of Plaintiff and the Class)

247. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 178 above as if fully set forth herein.

248. Plaintiff and Class Members have an interest, both equitable and legal, in the Private Information about them that was conveyed to, collected by, and maintained by Defendant and that was ultimately accessed or compromised in the Data Breach.

249. As a healthcare provider that collects and stores the Private Information of its patients, Defendant is in a position of trust and confidence *vis-à-vis* the individuals whose Private Information it collects and maintains, including Plaintiff and Class Members, and has a special relationship with such individuals.

250. Because of that special relationship, Defendant was provided with and stored private and valuable Private Information pertaining to Plaintiff and Class Members, which Defendant was required to maintain in confidence.

251. Plaintiff and the Class provided Defendant with their personal and confidential Private Information under both the express and/or implied agreement of Defendant to limit the use and disclosure of such Private Information through reasonable and adequate information security measures.

252. Defendant owed duties to Plaintiff and Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Private Information

in Defendant's possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

253. Defendant had an obligation to maintain the confidentiality of Plaintiff's and the Class Members' Private Information.

254. Plaintiff and Class Members have a privacy interest in their personal health matters, and Defendant had a duty not to disclose confidential medical information and records concerning its patients.

255. As a result of the parties' relationship, Defendant had possession and knowledge of confidential Private Information and confidential health data of Plaintiff and Class Members.

256. Plaintiff's and Class Members' Private Information is not generally known to the public and is confidential by nature.

257. Plaintiff and Class Members did not consent to nor authorize Defendant to release or disclose their Private Information to an unknown criminal actor.

258. Defendant breached the duties of confidence owed to Plaintiff and Class Members when Plaintiff's and Class Members' Private Information was disclosed to criminal hackers.

259. Defendant breached its duties of confidence by failing to safeguard Plaintiff's and Class Members' Private Information, including by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of patient information that resulted in the unauthorized access and compromise of Private Information; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and

adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the Data Breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to patients; (h) storing Private Information in an unencrypted and vulnerable manner, allowing its disclosure to hackers; and (i) making an unauthorized and unjustified disclosure and release of Plaintiff and the Class Members' Private Information to a criminal third party.

260. But for Defendant's wrongful breach of the duty of confidences owed to Plaintiff and Class Members, Plaintiff's and Class Members' privacy, confidences, and Private Information would not have been compromised.

261. As a direct and proximate result of Defendant's breach of Plaintiff's and the Class's confidences, Plaintiff and Class Members have suffered injuries, including, without limitation, (a) invasion of privacy; (b) lost or diminished value of their Private Information; (c) out-of-pocket and lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (d) emotional distress due to their Private Information's wrongful disclosure; and (e) the continued and certainly increased risk to their Private Information, which remains in Defendant's possession in unencrypted form and subject to further unauthorized disclosures, so long as Defendant fails to undertake appropriate and adequate measures to protect it.

262. Additionally, Defendant received payments from Plaintiff and Class Members, directly or indirectly, for DMES and services with the understanding that it would uphold its responsibilities to maintain the confidence of Plaintiff's and Class Members' Private Information.

263. Defendant breached the confidence of Plaintiff and Class Members when it failed to use reasonable or adequate data security measures to prevent the unauthorized release and

disclosure of Plaintiff's and Class Members' confidential Private Information in the Data Breach and, accordingly, it would be inequitable for Defendant to retain the benefit at Plaintiff and Class Members' expense.

264. As a direct and proximate result of Defendant's breaches of Plaintiff's and Class Members' confidence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

COUNT V
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

265. Plaintiff re-alleges and incorporates by reference herein all the allegations contained in paragraphs 1 through 179 above, as if fully set forth herein.

266. This count is in the alternative to the breach of implied contract count above.

267. Plaintiff and Class Members conferred a benefit on Defendant by way of paying and providing their Private Information to Defendant as part of Defendant's business as a healthcare provider.

268. The monies paid to Defendant were supposed to be used by Defendant, in part, to pay for the administrative and other costs of providing reasonable data security and protection to Plaintiff and Class Members.

269. Defendant failed to provide reasonable security, safeguards, and protections to the personal information of Plaintiff and Class Members, and as a result Defendant was overpaid.

270. Under principles of equity and good conscience, Defendant should not be permitted to retain the money because it failed to provide adequate safeguards and security measures to protect Plaintiff's and Class Members' personal information that they paid for but did not receive.

271. Defendant wrongfully accepted and retained these benefits to the detriment of Plaintiff and Class Members.

272. Defendant's enrichment at Plaintiff's and Class Members' expense is unjust.

273. As a result of Defendant's wrongful conduct, as alleged above, Plaintiff and the Class are entitled to restitution and disgorgement of profits, benefits, and other compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Anamari Laurentz, individually and on behalf of all others similarly situated, prays for judgment as follows:

A. An Order certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing her counsel to represent the Class;

B. Awarding Plaintiff and the Class damages that include applicable compensatory, actual, exemplary, and punitive damages, as allowed by law;

C. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

D. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

E. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

F. Awarding attorneys' fees and costs, as allowed by law,

G. Awarding prejudgment and post-judgment interest, as provided by law;

H. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and,

I. Any and all such relief to which Plaintiff and the Class are entitled.

JURY TRIAL DEMAND

Plaintiff hereby demands a trial by jury of all issues so triable.

Dated: November 4, 2024

Respectfully submitted,

By: /s/ Steven Sukert
Steven Sukert (NY Bar # 5690532)
Jeff Ostrow (*pro hac vice* forthcoming)
KOPELOWITZ OSTROW P.A.
One West Las Olas Blvd, Suite 500
Fort Lauderdale, FL 33301
Tel: (954) 525-4100
Fax: (954) 525-4300
sukert@kolawyers.com
ostrow@kolawyers.com

Counsel for Plaintiff and the Putative Class